Specification Amendment

Paragraph 0027 has been amended to refer to a "key handling unit." The association between the key handling unit and the TPM is set forth in original claim 32, for example, and would be understood by those familiar with the TCPA specification.

Withdrawal of the rejections and allowance of the claims are respectfully requested.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2125. In particular, if this response is not timely filed, then the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136 (a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2125.

I hereby certify that this correspondence is being deposited with the United States Post Office with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

June 5, 2007
(Date of Transmission)

Mary Ngo
(Name of Person Transmitting)

(Signature)

June 5, 2007
(Date)

Respectfully submitted,

Richard P. Berg
Attorney for the Applicant
Reg. No. 28,145
LADAS & PARRY
5670 Wilshire Boulevard,
Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile

Please amend the following paragraphs of the specification in the manner indicated:

[0011] The present invention relates to a computing platform which has a secure key-handling unit arranged to store a storage root key that forms the root node of a tree-structured node hierarchy the non-leaf nodes of which, other than the root node, each comprise, in encrypted form, a key used to encrypt the or each of its child nodes, and insecure storage for storing the hierarchy nodes other than the root node. The key-handling unit has (i) a memory for storing a current decryption-root key; (ii) a decrypted-access arrangement arranged to restrict decrypted access to the hierarchy nodes to those nodes decryptable by a chain of decryption rooted in said current decryption-root key; and (iii) a current-decryption-root setting arrangement for storing in said memory, in decrypted form, the key of a selected non-leaf node of said hierarchy to serve as said current decryption-root key, the current-decryption-root setting arrangement enabling the selected non-leaf node to be changed. ~~is based in part on the observation that previous platform history is irrelevant for software provided that all traces of previous software have been unloaded or existing software is benign (such as a protected compartment OS). In these cases, the operation of software is unaffected by software that previously executed on the platform. Software implementing a process may be considered to be "protected software", and the process a "protected process", when a mechanism expected to resist subversion provides a benign environment for that software/process to execute. That mechanism may, of course,~~

~~itself be a protected process. The decision to release secrets for use by software can therefore be made purely on the basis of knowing that the particular software about to be executed will be protected software. So, if a TPM "knows" that protected software is about to be started, the TPM can safely release the secrets for that protected software without knowing the history of previously-executed software as represented, for example, by PCR values.~~

[0012] In one embodiment, the setting arrangement is arranged to permit the selected non-leaf node, and thereby the decryption-root key, to be changed only upon a predetermined set of at least one condition being met. The at least one predetermined condition may comprise the receipt by the key handling unit of an authorization value indicative of particular digital data. In that case the authorization value is preferably a digest of a protected process associated with the node that is intended to be the new selected non-leaf node. In one embodiment, the at least one predetermined condition may comprise that a protected process, associated with the node that is intended to be the new selected non-leaf node, is about to be run by the computing platform. In another embodiment, the at least one predetermined condition may comprise that the key-handling apparatus is requested to change the selected non-leaf node by a root of trust of the computing platform.~~In the context of the TCPA architecture, a primary aspect of the present invention is concerned with arranging for secrets associated with a protected process to be released to the process by the TPM when the latter has received assurance that it is safe to do so. In a preferred embodiment, this~~

~~involves the use of a "dynamic root key" that is associated with the protected process to be run, the key itself forming part of the key hierarchy stored in Protected Storage. The dynamic root key will generally form the root of a hierarchy of objects associated with the protected process, with the cryptographic use of the key and the cryptographic protection processes of this hierarchy being carried out either by the TPM or by the protected process. The TPM makes the dynamic root key available for use only upon authorization by a trustable source (for example, a hardware root-of-trust or another protected process such as a protected compartment OS) that is responsible for ensuring that the process associated with the dynamic root key is protected (which may simply be because the protected process is the only process executing). The TPM uses any appropriate means, physical or virtual, to verify that the authorization came from such a trustable source. Preferably, the authorisation required by the TPM before making the dynamic root key available, is a digest of the protected process.~~

[0013] Preferably, upon start up of the computing platform, the node at the head of the hierarchy forms the selected non-leaf node. ~~Where the protected process hierarchy based on the dynamic root key is to be processed by the TPM, when the protected process is run (or about to be run), the associated dynamic root key is installed in the TPM to act as the root of a hierarchy of (external) data objects instead of the SRK. Access to parts of the key hierarchy that require ascent from the dynamic root key is prohibited.~~

[0014] Preferably the key-handling unit is arranged always to hold securely the node at the head of the hierarchy, in unencrypted form. ~~Where the protected-process hierarchy based on the dynamic root key is to be processed by the protected process itself, when the protected process is run (or about to be run) the dynamic root key is released to the protected process.~~

[0015] Although an embodiment of the present invention is described herein ~~has been outlined above~~ in the context of the TCPA architecture, it is of broader application.

[0016] ~~More particularly, according to one aspect of the present invention, there is provided a method of managing an hierarchy of nodes manipulated by processing apparatus, the method comprising a step of permitting access to a particular node of the hierarchy only after receiving a reliable indication that a mechanism expected to resist subversion will attempt to enforce appropriate access restrictions on that node and any descendent nodes.~~

[0017] ~~In a preferred embodiment of this method, the aforesaid mechanism is a protected process executing in a benign operating environment within the apparatus, the method further comprising using a trusted source to establish or initiate establishment of the mechanism and to generate said reliable indication accordingly.~~

[0018] ~~According to another aspect of the present invention, there is provided processing apparatus for~~

~~managing an hierarchy of nodes, the apparatus comprising an access-control arrangement for permitting access to a particular node of the hierarchy only upon receiving a reliable indication that a mechanism expected to resist subversion will attempt to enforce appropriate access restrictions on that node and any descendent nodes.~~

[0019] ~~According to yet another aspect of the present invention, there is provided processing apparatus comprising a key-handling unit for handling a tree-structured hierarchy in which each non-leaf node comprises a key used to encrypt the or each of its child nodes, the hierarchy including, below its top level, a node comprising a particular key associated with a protected process executable by the processing apparatus; the key-handling unit being arranged to make said particular key available for use in relation to the protected process upon receipt both of authorisation to do so and an indication that the authorisation is provided by a trusted source that is arranged to provide this authorisation, and to initiate or permit execution of said protected process, only after verifying the presence of a benign operating environment within the apparatus for said protected process.~~

[0020] ~~According to a further aspect of the present invention, there is provided processing apparatus comprising a key-handling unit for handling a tree-structured key hierarchy, the key-handling unit being arranged to treat a selected node of the hierarchy as the current root node such that those parts of the hierarchy that can only be reached by ascent from the current root~~

~~node are inaccessible, the key-handling unit including an arrangement for changing the node of the hierarchy serving as said current root node.~~

[0021] ~~According to a still further aspect of the present invention, there is provided a tree-structured key hierarchy with multiple nodes serving as root nodes dividing the hierarchy into different parts only accessible from corresponding root nodes.~~

[0027] FIG. 1 illustrates a ~~trusted~~ Trusted Platform Module (TPM) 10 with its normal Protected Storage data-object hierarchy 12 (also referred to below as a key hierarchy). The TPM's Storage Root Key (SRK) 11 resides permanently inside the TPM 10. The SRK 11 is used to encrypt ("wrap") keys K1-1, K1-2, K1-3 etc. that form the next level of the hierarchy. Key K1-1, which in this case is preferably a non-migratable key, itself wraps further keys K2-1, K2-2, etc. The hatched outer annulus around each key in the FIG. 1 key hierarchy 12 is a graphical indication that each key is wrapped (encrypted). A key in the hierarchy 12 can only be decrypted by the TPM 10 upon presentation to the latter of authorizations in respect of the ancestor keys in the hierarchy. A key-handling unit is part of the TPM 10. According to the TCPA specification, the TPM 10 has functionality for managing the Protected Storage hierarchy 12 -- this functionality is called a "key-handling unit" herein.